IN THE CLAIMS:

Please amend claims 1, 4, 8, 10-23, 37-42, and 44-46 as follows:

A1

1. (Once Amended) A method for certifying pieces of data in a system [with at least two levels of authorities]having authorities that certify data, comprising the steps of:

(a) presenting a piece of data requiring certification to a first [level] authority for inspection of a given property;

(b) if the piece of data passes the inspection of the first [level] authority, causing a [higher]second authority to receive an indication that the piece of data has passed the inspection of at least the first [level] authority;

(c) having the [higher]second authority issue a certificate that the piece of data possesses the given property, the second authority [certificate] including in the certificate a signature of the [higher]second authority [but not including]and the second authority omitting from the certificate a public key of the first [level] authority; and

(d) storing accountability information [in order to keep]that renders at least the first [level] authority accountable for pieces of data that the first [level] authority contributes to certify.

A2

4. (Once Amended) A method for certifying, according to claim 3, wherein the inspection by the first [level] authority includes identifying the presenting user.

A3

8. (Once Amended) A method for certifying, according to claim 1, wherein a certified public verification key of the [higher]second authority is sufficient to verify the certificate.

24

10. (Once Amended) A method for certifying, according to claim 9, wherein the [higher]second authority contributes additional data that is included in the certificate.

11. (Once Amended) A method for certifying, according to claim 1, wherein the accountability information [that is stored can be used to identify]identifies the first [level] authority.

12. (Once Amended) A method for certifying, according to claim 11, wherein the accountability information [that is stored] is a digital signature of the first [level] authority.

14 ~~13~~. (Once Amended) A method for certifying, according to claim 11, wherein the accountability information [that is stored] indicates the name of the first [level] authority.

24

16 ~~14~~. (Once Amended) A method for certifying, according to claim 1, wherein at least a portion of the accountability information [that is stored] is stored in the certificate.

17 ~~15~~. (Once Amended) A method for certifying, according to claim 16 ~~14~~, wherein all of the accountability information [that is stored] is stored in the certificate.

18 ~~16~~. (Once Amended) A method for certifying, according to claim 1, wherein the certificate includes a digital signature of the first [level] authority.

15 ~~17~~. (Once Amended) A method for certifying, according to claim 11, wherein the certificate includes a digital signature of the first [level] authority.

25

13 ~~18~~. (Once Amended) A method for certifying, according to claim 12, wherein the certificate includes a digital signature of the first [level] authority.

19. (Once Amended) A method for certifying, according to claim 1, further comprising the step of:

(e) the [higher level]second authority [causes]causing additional information to be saved which, when combined with the accountability information [that is stored], proves that the first [level] authority contributed to certification of the piece of data.

14

20. (Once Amended) A method for certifying, according to claim 1, further comprising the step of:

(e) a witness causing information to be saved that indicates that the first [level] authority contributed to certification of the piece of data, wherein the information that is saved by the witness is separate from the accountability information and wherein the accountability information [that is stored] is stored in a way to indicate the identity of the witness.

21. (Once Amended) A method for certifying, according to claim 20, wherein the information caused to be saved by the witness includes a portion of a digital signature and the accountability information [that is stored] includes an other portion of [a]the digital signature.

22. (Once Amended) A method for certifying, according to claim 21, wherein the portions of the digital signature [can be combined to], when combined, prove that the first [level] authority

26

contributed to certification of the piece of data.

23. (Once Amended) A method for certifying public keys where there are a plurality of authorities $A_1, \ldots, A_n$ that certify data, where each $i<n$ authority A_i [can]is configured to send authority A_{i+1} authenticated messages [so] that are verifiable by [at least] A_{i+1} [can be sure that these messages]as having genuinely come from A_i, and authority A_n has a signing key SK_n and an associated certified public key, PK_n, the method comprising the steps of:

a4

(a) having a verification key PK_U presented to authority A_1;

(b) having authority A_1 verify, by means of a predetermined procedure, that PK_U possesses some properties out of a set of given properties;

(c) for all $i<n$, having authority A_i send authority A_{i+1} a message indicating that PK_U has been verified to possess the given properties;

(d) having A_n issue a certificate for PK_U, [the certificate] A_n including in the certificate a signature provided using SK_n [but not including]and A_n omitting from the certificate a public key of at least one authority A_j for some $j<n$; and

(e) storing accountability information [to keep]that renders A_j accountable for keys that A_j contributes to certify.

37. (Once Amended) A method for certifying, according to claim 23, wherein the accountability information [that is stored can be used to identify]identifies A_j.

a5

38. (Once Amended) A method for certifying, according to claim 37, wherein the accountability information [that is stored] is a digital signature of A_j.

27

39. (Once Amended) A method for certifying, according to claim 37, wherein the accountability information [that is stored] indicates the name of A_j.

40. (Once Amended) A method for certifying, according to claim 23, wherein at least a portion of the accountability information [that is stored] is stored in the certificate.

a5

41. (Once Amended) A method for certifying, according to claim 40, wherein all of the accountability information [that is stored] is stored in the certificate.

42. (Once Amended) A method for certifying, according to claim 23, further comprising the step of:

(f) an authority A_k causing additional information to be saved which, when combined with the accountability information [that is stored], proves that A_j contributed to the certification of PK_U.

44. (Once Amended) A method for certifying, according to claim 23, further comprising the step of:

a6

(f) a witness causing information to be saved that indicates that A_j contributed to the certification of PK_U, wherein the information that is saved is separate from the accountability information and the accountability information [that is stored] indicates the identity of the witness.

45. (Once Amended) A method for certifying, according to claim 44, wherein the information that is caused to be saved by the witness includes a portion of a digital signature and the

27